MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
EJÉRCITO NACIONAL
DIRECCION DE PERSONAL

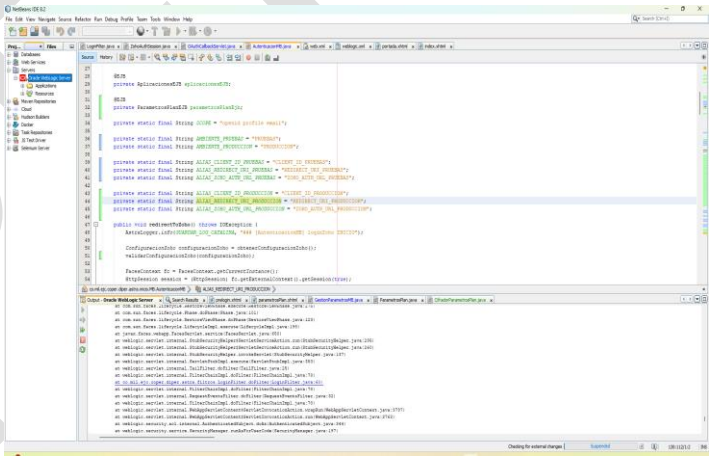
INFORME DE GESTIÓN No. 05

Bogotá (Cundinamarca), JUNIO 2026

1. No. DEL CONTRATO	396-CENACPERSONAL-2026
2. FECHA SUSCRIPCIÓN CONTRATO	**29 DE ENERO DE 2026**
3. PÓLIZA DE SEGUROS	No. De la Póliza No. **360 47 994000063638** Entidad que expide la póliza: Aseguradora Solidaria de Colombia Fecha del certificado de aprobación de la Póliza: 04-FEB-2026 Aprobado por: TC. LIBARDO CERQUERA PASTRANA
4. CRP	No.29726 de fecha 03 de febrero del 2026 Fecha expedición: 03 de febrero del 2026 Unidas/Sub-unidad ejecutora CENAC-PERSONAL Dependencia: DIPER Posición catálogo de gasto: (A-02.02.02.008.003-13) 10CSF Fuente: NACIÓN Recurso 10 Valor: $56.700.000.00
5. FECHA INICIO EJECUCIÓN CONTRACTUAL	**5 DE FEBRERO DE 2026**
6. CONTRATISTA	Nombre completo: ERICK ENRIQUE SANCHEZ DIAZ Identificación1´023.886.053 Nacionalidad Colombiana Dirección Carrera 7 #31-21 Sur Bogotá Teléfono de contacto 3163551894 E-mail de contacto: erick.eagle@gmail.com
7. SUPERVISOR	Nombre completo: CT. DAVID RODRIGUEZ CABRERA Cargo: Oficial Administrador Informático Resolución de nombramiento: Resolución No.00000412 fechada 19 de ENERO de 2026. Teléfono de contacto 3128792902 E-mail de contacto: david.rodriguez@buzonejercito.mil.co
8. OBJETO CONTRACTUAL	PRESTAR LOS SERVICIOS PROFESIONALES COMO INGENIERO DE SISTEMAS CON EXPERIENCIA EN DESARROLLO DE SOFTWARE BAJO LA PLATAFORMA DE ORACLE FORMS & REPORTS Y DESARROLLO EN PL/SQL ORACLE
9. OBLIGACIONES CONTRACTUALES	OBLIGACIONES ESPECIFICACIONES 1. Realizar levantamiento, análisis y socialización de los requerimientos y mejoras de los sistemas de información bajo la tecnología java. 2. Realizar verificación y ajuste en los datos, los formularios, los reportes de los sistemas de información bajo la tecnología java. 3. Realizar propuestas de solución de acuerdo a los requerimientos para ajustes de presentación de datos en los diferentes módulos reportes de los sistemas de información bajo la tecnología java. 4. Diseñar o desarrollar formularios y reportes para el manejo de la información de acuerdo a la verificación de los requerimientos.

DIPER

	5. Realizar todos los demás ajustes adicionales a los formularios, reportes, procesos y procedimientos requeridos por el supervisor del contrato cuando se presente la necesidad inmediata relacionada con el funcionamiento de los sistemas de información bajo la tecnología java. OBLIGACIONES CONTRACTUALES GENERALES: ✓ Observar durante el tiempo de ejecución del contrato, buena disposición y actitud favorable hacia el trabajo, respeto hacia sus compañeros y miembros del Ejército Nacional, al igual que la aplicación permanente de principios y valores propios de la institución militar. ✓ Dar estricto cumplimiento durante todas sus actuaciones, al marco normativo correspondiente a la integridad, trasparencia y lucha contra la corrupción. ✓ Guardar y mantener la debida reserva y confiabilidad frente a los temas y asuntos tratados y conocidos dentro del desarrollo y ejecución del presente contrato, reserva que se hará extensiva a los derechos de autor que de los mismos se derive. ✓ Aplicar medidas pasivas de seguridad con la documentación según clasificación con el fin de evitar la fuga de información de acuerdo con la normatividad vigente. ✓ De conformidad con el artículo 3 del Decreto 2609 de 2012, el contratista será responsable por la gestión documental de las actividades realizadas durante la ejecución del Contrato, presentando en el cronograma de actividades y en su informe de forma mensual el barrido de los documentos en físico y el término del almacenamiento del Orfeo hasta el archivo de los documentos. ✓ El contratista debe custodiar y a la terminación del presente contrato devolver los insumos, suministros, herramientas, dotación, implementación, inventarios y/o materiales que sean puestos a su disposición para la prestación del servicio objeto de este contrato. ✓ Entregar al final de la prestación del servicio, backup de la información producto ejecución del contrato. ✓ El contratista autoriza al MDN – EJÉRCITO NACIONAL a realizar los estudios de seguridad, comprobación de lealtad, realización de los exámenes de poligrafía y pruebas sicométricas antes y durante la contratación. ✓ Las demás obligaciones establecidas en el estudio previo, documento que el contratista declara conocer, y que hace parte del presente contrato. ✓ Las demás obligaciones que se deriven del objeto del contrato. PARÁGRAFO PRIMERO: Independencia del Contratista. El Contratista es independiente del Ministerio de Defensa – Ejército Nacional, y en consecuencia, el Contratista no es su representante, agente o mandatario. El Contratista no tiene la facultad de hacer declaraciones, representaciones o compromisos en nombre del Ministerio de Defensa – Ejército Nacional, ni de tomar decisiones o iniciar acciones que generen obligaciones a su cargo

	No	No. Obligación	No. Radicado	Descripción
10. DOCUMENTOS QUE SOPORTAN EL CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES	1	1,2,3,4,5	No Aplica	1. Realizar levantamiento, análisis y socialización de los requerimientos y mejoras de los sistemas de información bajo la tecnología java. **1. AVANCE ELIMINACIÓN VALORES SENSIBLES** Se avanzó en la eliminación de valores sensibles quemados en código fuente para la integración de ASTRA con Zoho. Las variables de configuración de pruebas y producción, como `CLIENT_ID`, `CLIENT_SECRET`, `REDIRECT_URI`, `ZOHO_AUTH_URL` y `TOKEN_ENDPOINT`, fueron trasladadas conceptualmente al módulo de parámetros del sistema, permitiendo que la aplicación consulte dinámicamente la configuración según el ambiente detectado. Este ajuste reduce la exposición de credenciales en repositorio, facilita el despliegue por ambiente y evita que los cambios de configuración OAuth dependan de recopilación del artefacto.  Imagen 1.
	2	1,2,3,4,5	No Aplica	2. Realizar verificación y ajuste en los datos, los formularios, los reportes de los sistemas de información bajo la tecnología java. **2. REVISIÓN TÉCNICA DEL DOCUMENTO DE VULNERABILIDADES DE ASTRA** Se realizó la revisión técnica del documento de vulnerabilidades de ASTRA, tomando como base el análisis original y las soluciones propuestas para los hallazgos reportados sobre encabezados HTTP, políticas de seguridad de contenido, exposición de recursos, configuración TLS, manejo de errores, validación de accesos y protección contra divulgación de información sensible. A partir de esta revisión se clasificaron los controles que ya cuentan con una solución implementada o parcialmente cubierta en la aplicación, y se identificaron los

DIPER

ajustes que requieren validación adicional en código fuente, configuración del servidor WebLogic, proxy reverso, balanceador o parámetros de despliegue.

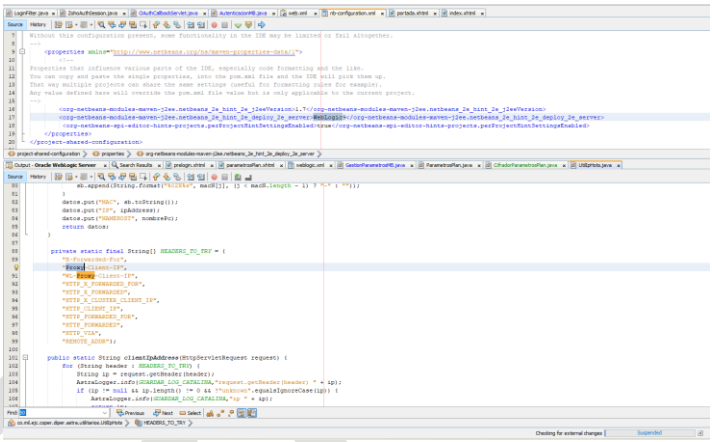


Imagen 2.

2.1. REVISIÓN TRATAMIENTO DE ENCABEZADOS

Se revisó el tratamiento de encabezados de seguridad HTTP, especialmente los relacionados con `X-XSS-Protection`, `X-Frame-Options`, `Content-Security-Policy`, `X-Content-Type-Options` y `Referrer-Policy`. La solución propuesta mediante una clase `Filter` es técnicamente válida y permite centralizar la inclusión de encabezados en todas las respuestas de la aplicación. Sin embargo, la implementación debe validarse en profundidad para confirmar que el filtro esté registrado efectivamente en `web.xml` o mediante anotación reconocida por el contenedor, que aplique sobre `/*`, que no sea sobrescrito por WebLogic, Oracle HTTP Server, balanceador o Alteon, y que la política CSP no afecte componentes dinámicos de PrimeFaces como AJAX, diálogos, calendarios, tablas, filtros y scripts generados por JSF.

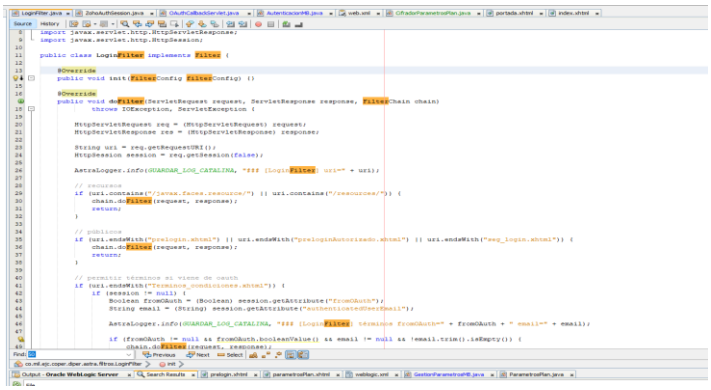


Imagen 3.

2.2. CLASE DE FILTER

En relación con la clase `Filter`, el ajuste se considera cubierto solo de forma parcial mientras no se verifique en ambiente real que todos los encabezados aparezcan en las respuestas finales entregadas al navegador. La revisión debe incluir páginas públicas, páginas autenticadas, recursos JSF, recursos estáticos, respuestas 302, respuestas 403 y respuestas 404. Adicionalmente, debe revisarse si la política `X-Frame-Options` se maneja como `SAMEORIGIN` desde la aplicación o como `DENY` desde infraestructura, ya que ambas pueden cerrar el hallazgo de clickjacking, pero tienen efectos diferentes si en algún punto ASTRA requiere incrustar contenido propio en iframe. También debe evitarse duplicidad o contradicción entre `X-Frame-Options` y `Content-Security-Policy frame-ancestors`.

2.3. IMPLEMENTACIÓN CSP

Para CSP, la implementación requiere una revisión adicional de compatibilidad con PrimeFaces. Una política demasiado estricta con `script-src 'self'` puede romper componentes generados dinámicamente por JSF/PrimeFaces, mientras que una política con `unsafe-inline` y `unsafe-eval` puede seguir siendo reportada por herramientas de análisis como una configuración débil. El cierre técnico debe plantearse por etapas: primero aplicar una CSP compatible que reduzca exposición, luego identificar JavaScript embebido propio, migrar scripts personalizados a archivos externos bajo `/resources`, revisar eventos `onclick` o scripts inline en XHTML y posteriormente evaluar la activación de `primefaces.CSP` si la versión utilizada lo soporta correctamente sin afectar la operación.

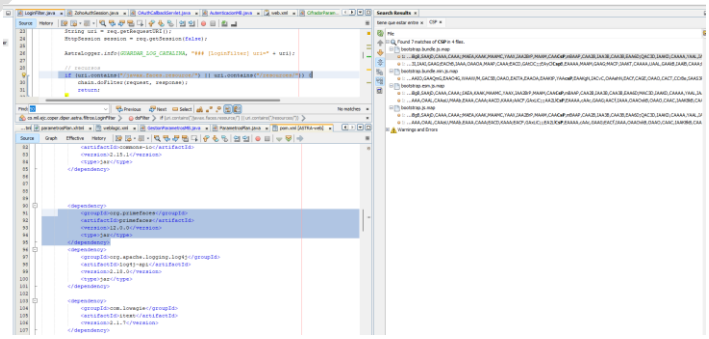
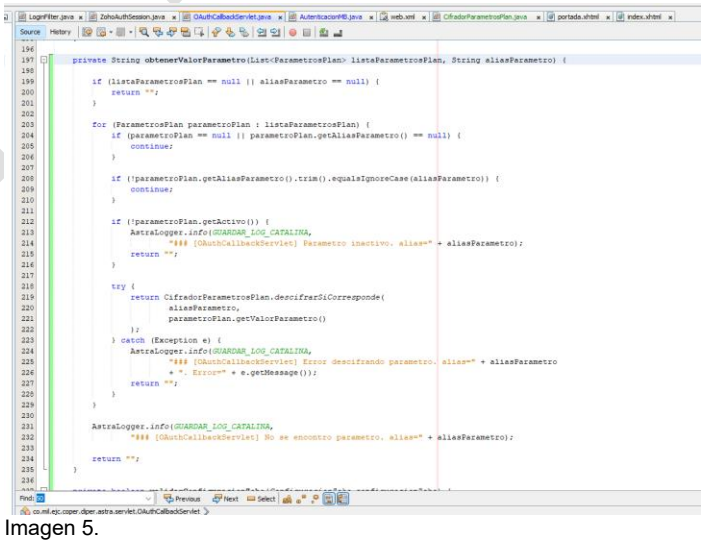


Imagen 4.

2.4. HALLAZGO HSTS

El hallazgo de HSTS no debe considerarse completamente cerrado únicamente con un filtro Java si ASTRA se encuentra detrás de un proxy, balanceador o terminador SSL. Si

				WebLogic recibe la petición como HTTP interno, `request.isSecure()` puede retornar falso y el encabezado `Strict-Transport-Security` no será agregado por la aplicación. Por esta razón, el control debe validarse preferiblemente en el componente que termina HTTPS, como balanceador, proxy reverso, Oracle HTTP Server o WebLogic frontal. La respuesta pública final debe incluir `Strict-Transport-Security: max-age=31536000; includeSubDomains`, siempre que previamente se confirme que los subdominios involucrados soportan HTTPS correctamente.
	3	1,2,3,4,5	No Aplica	3. Realizar propuestas de solución de acuerdo a los requerimientos para ajustes de presentación de datos en los diferentes módulos reportes de los sistemas de información bajo la tecnología java. **3. ACTUALIZÓ EL ENFOQUE DE AUTENTICACIÓN OAUTH** Se actualizó el enfoque de autenticación OAuth para que la configuración de Zoho sea construida dinámicamente desde parámetros y no desde constantes internas de la clase. El flujo mantiene controles relevantes como generación de `state`, almacenamiento temporal en sesión, validación del `state` recibido en el callback, limpieza de atributos previos de autenticación, extracción del correo desde el `id_token` y redirección controlada al flujo de aceptación de términos. Este comportamiento mejora la separación entre lógica de autenticación, configuración por ambiente y administración segura de credenciales.  Imagen 5.
	4	1,2,3,4,5	No Aplica	4. Diseñar o desarrollar formularios y reportes para el manejo de la información de acuerdo a la verificación de los requerimientos. **4. DEFINICIÓN DEL CIFRADO DE PARÁMETROS SENSIBLES EN LA ADMINISTRACIÓN INTERNA DE ASTRA**

DIPER

Se definió el cifrado de parámetros sensibles en la administración interna de ASTRA, específicamente para los alias asociados a la configuración OAuth de Zoho en pruebas y producción. El ajuste impacta los métodos de creación y edición de parámetros, de tal manera que, cuando el alias corresponde a un valor sensible, el dato se almacena cifrado en base de datos y solo se descifra en tiempo de ejecución cuando la aplicación necesita consumirlo. Esta mejora fortalece la protección de secretos, especialmente `CLIENT_SECRET`, tokens de configuración y endpoints críticos, evitando que queden visibles en texto.

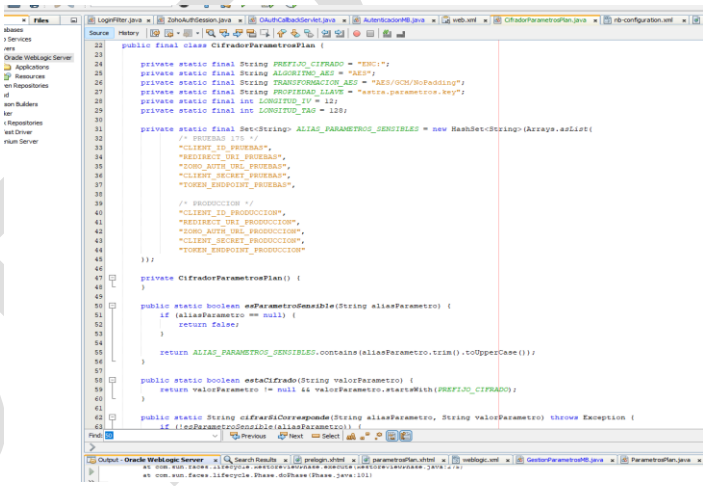
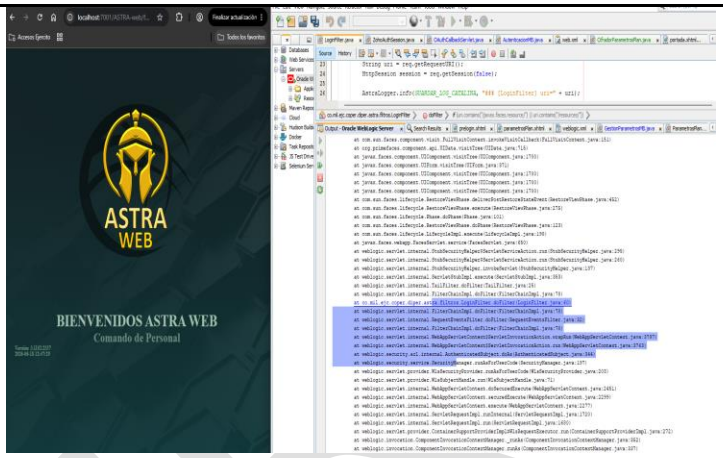
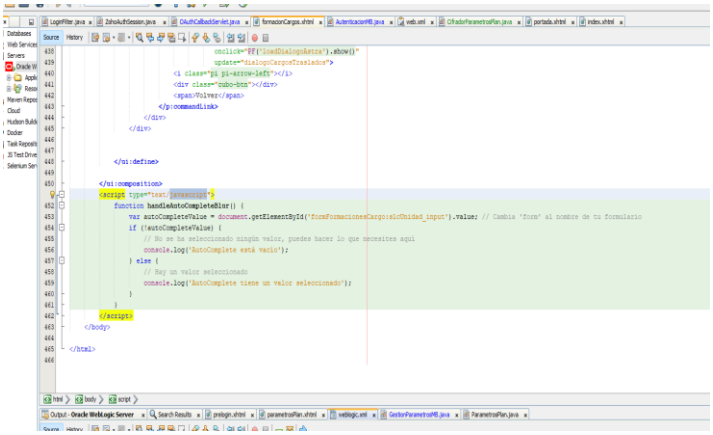


Imagen 6.

4.1. HALLAZGOS DE `RESOURCEFINDER`

Para los hallazgos de `ResourceFinder` y `FrontPageChecks`, se evidenció que varias rutas probadas por el escáner responden con `404 Not Found` o son redirigidas hacia la página de autenticación. Aunque esto puede indicar falso positivo cuando no existe exposición real de directorios, el comportamiento debe ajustarse cuidadosamente para que las rutas inexistentes no devuelvan contenido de login con código HTTP 200 ni respuestas que puedan ser interpretadas como existencia del recurso. El ajuste pendiente en código fuente consiste en interceptar rutas inexistentes o patrones típicos de escaneo, como `_vti_bin`, `.git`, `backups`, `tests`, `admin.exe` o `nimda.dll`, y responder con `sendError(HttpServletResponse.SC_NOT_FOUND)` o `403` cuando corresponda, sin redireccionarlas a `prelogin.xhtml`.

				 Imagen 7.
	5	1,2,3,4,5	No Aplica	5. Realizar todos los demás ajustes adicionales a los formularios, reportes, procesos y procedimientos requeridos por el supervisor del contrato cuando se presente la necesidad inmediata relacionada con el funcionamiento de los sistemas de información bajo la tecnología java. **5. HALLAZGO `JAVASCRIPTLEAKS`** El hallazgo `JavaScriptLeaks` se clasifica como un punto de endurecimiento y calidad de código, especialmente cuando proviene de librerías internas de PrimeFaces, jQuery o componentes de terceros que no deben modificarse directamente. Para el código propio de ASTRA sí corresponde revisar archivos JavaScript bajo recursos de la aplicación y agregar `"use strict";` donde sea viable, corregir variables globales accidentales, evitar funciones embebidas en XHTML y mover lógica cliente a archivos externos versionados. Este ajuste mejora mantenibilidad y reduce hallazgos repetitivos, aunque no representa por sí solo una vulnerabilidad crítica explotable.  Imagen 8.

5.1. `INJECTION SINKS`

Para `Injection Sinks`, se requiere revisión de código fuente en consultas, parámetros recibidos desde vistas JSF, servlets, filtros y métodos que construyan SQL dinámico, JavaScript, HTML o URLs. Debe confirmarse que las consultas a base de datos utilicen parámetros enlazados, `PreparedStatement`, `TypedQuery`, `createNativeQuery` parametrizado o procedimientos controlados, evitando concatenación directa de valores ingresados por usuario. En las salidas hacia XHTML debe mantenerse el escape por defecto de JSF y evitar `escape="false"` salvo casos plenamente controlados. Este punto no queda cerrado solo con encabezados de seguridad, porque requiere revisión de código fuente y pruebas específicas sobre entradas de usuario.

5.2. PRIMEFACES

PrimeFaces tiene soporte oficial para **Content Security Policy**. La documentación indica que CSP se activa con el parámetro de contexto:

XML

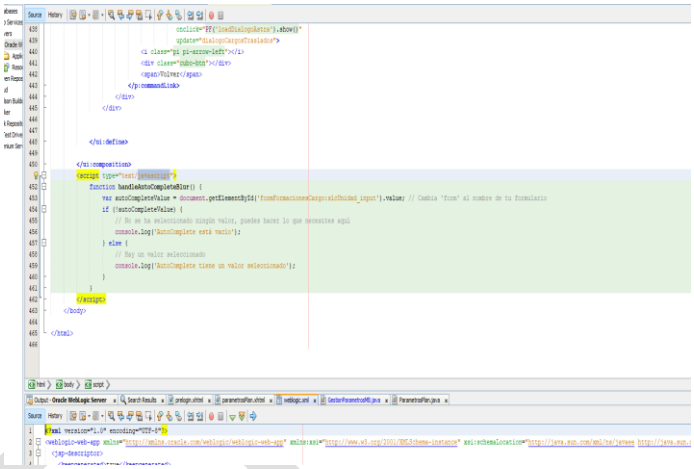
```xml
<context-param>
    <param-name>primefaces.CSP</param-name>
    <param-value>true</param-value>
</context-param>
```

La documentación aclara

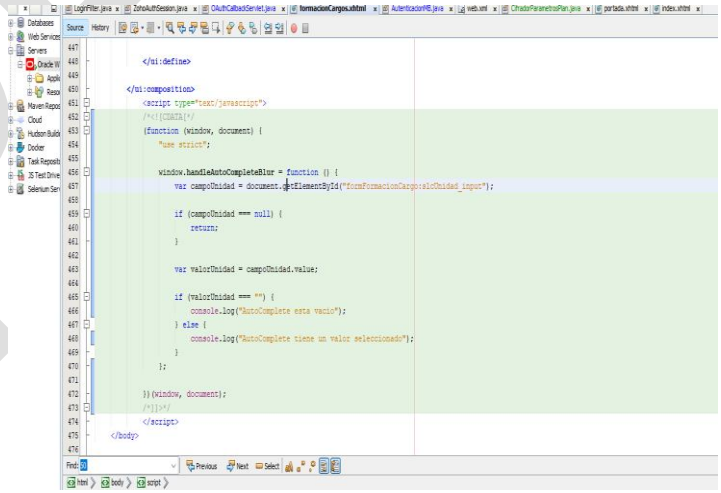
(https://primefaces.github.io/primefaces/jsdocs/modules/src_PrimeFaces.PrimeFaces.csp.html): PrimeFaces no puede conocer todos los usos de JavaScript personalizados en cada aplicación, por lo cual permite configurar una política personalizada mediante primefaces.CSP_POLICY. Esto significa que el framework ayuda a controlar los scripts que genera o procesa, pero no exonera la revisión del JavaScript propio escrito a mano en los XHTML.

Para `AnonymousAccessType`, el control debe validarse contra rutas públicas, recursos JSF, servlets, páginas XHTML, archivos estáticos y endpoints auxiliares. ASTRA ya cuenta con flujo de prelogin, autenticación OAuth y validación de sesión, pero debe verificarse que no existan páginas internas accesibles de forma directa sin sesión válida. El ajuste pendiente consiste en revisar filtros de autenticación, reglas en `web.xml`, navegación JSF y rutas de servlets para garantizar que únicamente queden públicas las pantallas necesarias de prelogin, callback OAuth, recursos estáticos requeridos para autenticación y páginas explícitamente autorizadas.

DIPER



Antes
Imagen 9.



Después
Imagen10.

5.3. `**SSLTLSV11**`

Para `SSLTLSv11`, el cierre no depende principalmente del código fuente de ASTRA sino de la configuración del servidor y la infraestructura. Debe validarse que WebLogic, JVM, proxy o balanceador tengan deshabilitados TLS 1.0 y TLS 1.1, dejando como mínimo TLS 1.2 y, si la plataforma lo permite, TLS 1.3. En WebLogic/JVM se debe revisar la configuración de protocolos mínimos y suites criptográficas, así como la compatibilidad con clientes institucionales. Este control debe

cerrarse con evidencia de configuración y prueba externa de negociación TLS.

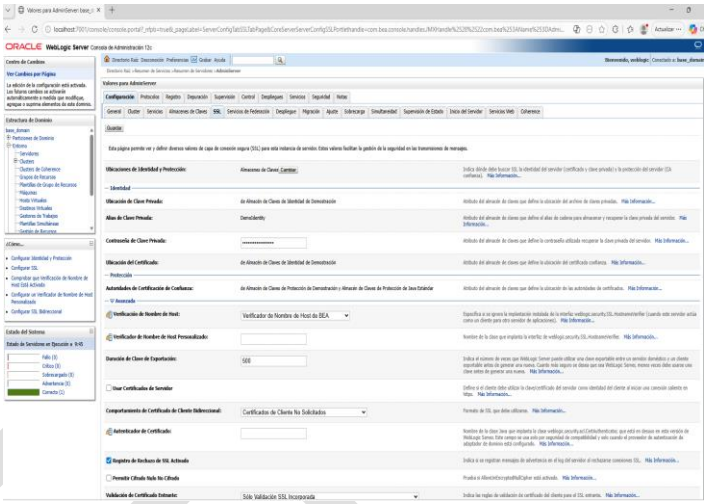


Imagen 11.

5.4. INCORPORACIÓN DEL CONTROL OPERATIVO

Se incorporó el control operativo de las tareas mediante Trello, organizando el trabajo en un flujo de seguimiento por listas. En el `BackLog` se registran los temas identificados, requerimientos técnicos, hallazgos y mejoras internas pendientes de análisis. En la lista `TO-DO` quedan las tareas priorizadas para iniciar desarrollo. En `DOING` se ubican las actividades que se encuentran en implementación. En `TESTING` se registran los ajustes ya subidos a GitLab, desde donde se realiza revisión de código, integración de cambios, validación técnica y generación del desplegable para pruebas y producción. Finalmente, en `DONE` se consolidan los temas ya revisados, integrados y cerrados funcional o técnicamente.

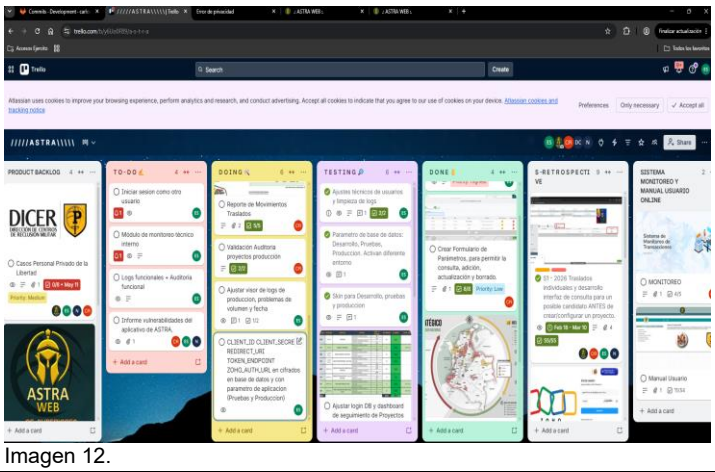
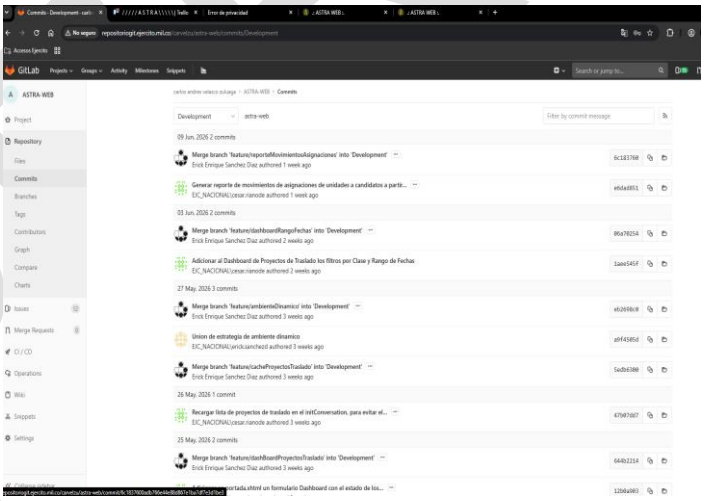


Imagen 12.

					5.5. CICLO DE INTEGRACIÓN En el ciclo de integración se mantiene la trazabilidad entre las tareas priorizadas, los cambios aplicados en código fuente y los desplegables generados. Los ajustes relacionados con parámetros seguros, configuración dinámica de Zoho, cifrado de valores sensibles, filtros de encabezados de seguridad, revisión de rutas inexistentes, configuración de respuestas HTTP y endurecimiento general deben quedar asociados a sus respectivas tarjetas de Trello y a los commits correspondientes en GitLab. Esto permite controlar el avance real, separar los puntos cerrados de los parcialmente implementados y dejar evidencia del paso de cada mejora por revisión, integración, pruebas y generación de artefactos.  Imagen 13.
11. CONSTANCIAS	Dejo constancia que, durante el plazo de ejecución del contrato, no se han configurado los presupuestos legales del contrato laboral y que he gozado de plena autonomía para ejecutar las obligaciones contractuales relacionadas en el contrato. Así mismo, tanto el/la suscrito/a y el Ministerio de Defensa – Ejército Nacional – Unidad Ejecutora ha dado cumplimiento a las obligaciones legales y contractuales registradas en el contrato.				

Para constancia se firma en, **(Bogotá),** en el mes de **JUNIO 2026**

FIRMA CONTRATISTA
POST FIRMA: PS. ERICK ENRIQUE SANCHEZ DIAZ
CC.:1´023.886.053
Contrato No. 396-CENACPERSONAL-2026